

# Maximum Devices Configurations

## Networking Concepts and Commands

### Router Commands

```
hostname [Router_Name]
banner motd # Entering restricted area! #
service password-encryption
enable secret [enable_password]
line con 0
password [console_password]
login
line vty 0 4
password [vty_password]
login
logging synchronous
exec-timeout [minutes] [seconds]
no ip domain-lookup
interface [interface_id]
ip address [ip_address] [subnet_mask]
description [description_text]
ip route [destination_network] [subnet_mask] [next_hop_ip]
ip route 192.168.2.0 255.255.255.0 192.168.1.1
ip route 0.0.0.0 0.0.0.0 [next_hop_ip]
ip route 0.0.0.0 0.0.0.0 192.168.1.1
router rip
version 2
network [network_number]
```

router rip

version 2

network 192.168.1.0

access-list [number] permit [source] [wildcard\_mask]

access-list 10 permit 192.168.1.0 0.0.0.255

access-list [number] permit [protocol] [source] [wildcard\_mask] [destination] [wildcard\_mask]

access-list 100 permit tcp 192.168.1.0 0.0.0.255 any

ip domain-name [domain]

crypto key generate rsa

line vty 0 4

transport input ssh

ip domain-name example.com

crypto key generate rsa

line vty 0 4

transport input ssh

ip dhcp pool [pool\_name]

network [network\_address] [subnet\_mask]

default-router [router\_ip]

dns-server [dns\_ip]

ip dhcp pool MyDHCPPool

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 8.8.8.8

interface [interface\_id]

encapsulation ppp

ppp chap hostname [username]

ppp chap password [password]

interface Serial0/0

encapsulation ppp

ppp chap hostname user123

ppp chap password MyPPPPassword

interface tunnel [number]

ip address [ip\_address] [subnet\_mask]

tunnel source [source\_ip]

tunnel destination [destination\_ip]

interface tunnel 1

ip address 10.1.1.1 255.255.255.0

```
tunnel source 192.168.1.1
tunnel destination 192.168.2.1
ip nat inside source static [local_ip] [global_ip]
ip nat inside source static 192.168.1.10 203.0.113.1
policy-map [policy_name]
class [class_name]
bandwidth [amount]
policy-map MyQoSPolicy
class MyTrafficClass
bandwidth 1000
ip sla [operation_number]
icmp-echo [ip_address]
frequency [seconds]
ip sla 1
icmp-echo 8.8.8.8
frequency 30
ip ospf cost 4
```

---

## Switch Commands

```
hostname [Switch_Name]
banner motd # Entering restricted area! #
service password-encryption
enable secret class1235
line con 0
password cisco12345
login
line vty 0 4
password cisco12345
login
logging synchronous
exec-timeout 4 0
no ip domain-lookup
```

---

```
vtp mode server  
vtp domain [domain_name]  
vtp password [password]
```

```
vtp mode server  
vtp domain MyVTPDomain  
vtp password VTPPassword123
```

```
interface [interface_id]  
switchport mode access  
switchport access vlan [vlan_id]
```

```
interface GigabitEthernet0/1  
switchport mode access  
switchport access vlan 10
```

```
switchport mode access  
switchport mode dynamic auto  
switchport mode dynamic desirable  
switchport mode trunk  
switchport nonegotiate
```

```
interface GigabitEthernet0/2  
switchport mode access  
switchport mode dynamic auto  
switchport mode dynamic desirable  
switchport mode trunk  
switchport nonegotiate
```

```
spanning-tree mode rapid-pvst  
interface [interface_id]  
spanning-tree link-type point-to-point
```

```
spanning-tree mode rapid-pvst  
interface GigabitEthernet0/3  
spanning-tree link-type point-to-point
```

```
interface port-channel [number]  
switchport mode trunk
```

```
interface port-channel1  
switchport mode trunk
```

```
standby [group_number] ip [virtual_ip]  
standby [group_number] priority [priority_value]
```

```
standby [group_number] preempt
```

```
standby 1 ip 192.168.1.254
```

```
standby 1 priority 100
```

```
standby 1 preempt
```

```
router eigrp [asn]
```

```
network [network_address]
```

```
router eigrp 100
```

```
network 192.168.1.0
```

```
access-list [number] permit [protocol] [source] [wildcard] [destination] [wildcard]
```

```
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
```

```
snmp-server community [community_string] ro
```

```
snmp-server community MyCommunityString ro
```

---

Okay, I can absolutely organize these commands by whether they are typically configured on **Routers** or **Switches**.

This separation will make it clearer where each set of commands applies within a network.

### Important Considerations for Organization:

- **Some Overlap:** A few commands (like `hostname`, `banner motd`, `service password-encryption`, `enable secret`, `line con 0`, `line vty 0 4`, `logging synchronous`, `exec-timeout`, `no ip domain-lookup`) are fundamental to *both* routers and switches. I'll list these under a "Common Core Commands" section for clarity, as they apply to both device types.
- **Context for "Router on a Stick":** While "Router on a Stick" is a router function, it heavily involves switch configuration for trunking. I'll put the *router* commands in the router section and the *switch* commands in the switch section, linking them by topic.
- **ACLs:** ACLs can be applied to both router and switch interfaces (specifically, Switched Virtual Interfaces - SVIs on switches). I'll place the ACL *definition*

under Routers (as routers are typically the primary point of ACL application) and note that they can be applied to SVIs on switches in the switch section.

- **Verification Commands:** I will largely omit `show` and `debug` commands from this organized list to keep it focused on *configuration*. Assume that for every configuration command, there's a corresponding `show` command (e.g., `show ip route` for `ip route` ).
- 

## Networking Concepts and Commands: Organized by Device

---

### A. Common Core Commands (Applicable to Both Routers & Switches)

These commands are fundamental for initial device setup, security, and management.

- **Basic Device Identification & Security:**
  - `hostname [Device_Name]`
  - `banner motd # Entering restricted area! #`
  - `service password-encryption`
  - `enable secret [enable_password]` (e.g., `enable secret class1235` )
- **Console Line Configuration:**
  - `line con 0`
  - `password [console_password]` (e.g., `password cisco12345` )
  - `login`
  - `logging synchronous`
  - `exec-timeout [minutes] [seconds]` (e.g., `exec-timeout 4 0` )
- **Virtual Terminal Lines (Telnet/SSH Access):**
  - `line vty 0 4`
  - `password [vty_password]` (e.g., `password cisco12345` )
  - `login`

- `exec-timeout [minutes] [seconds]`
  - **General Utility:**
    - `no ip domain-lookup` (prevents device from trying to resolve mistyped commands as domain names)
- 

## B. Router Commands

These commands are primarily used for routing, WAN connectivity, advanced security, and specific services typically run on routers.

### I. Interface Configuration & Addressing

- **Interface Access:**
  - `interface [interface_id]` (e.g., `interface GigabitEthernet0/0` , `interface Serial0/0` )
- **IPv4 Addressing:**
  - `ip address [ip_address] [subnet_mask]`
  - `no shutdown` (to activate the interface)
- **Interface Description:**
  - `description [description_text]`

### II. Routing Protocols

- **Static Routes:**
  - `ip route [destination_network] [subnet_mask] [next_hop_ip]` (e.g., `ip route 192.168.2.0 255.255.255.0 192.168.1.1` )
  - `ip route 0.0.0.0 0.0.0.0 [next_hop_ip]` (Default Route / Gateway of Last Resort, e.g., `ip route 0.0.0.0 0.0.0.0 192.168.1.1` )
- **RIPv2:**
  - `router rip`
  - `version 2`
  - `network [network_number]` (e.g., `network 192.168.1.0` )

- `no auto-summary` (highly recommended for classless routing)
- `passive-interface [interface_id]` (optional, to prevent updates on certain interfaces)
- **EIGRP:**
  - `router eigrp [asn]` (Autonomous System Number, e.g., `router eigrp 100` )
  - `network [network_address] [wildcard_mask]` (e.g., `network 192.168.1.0 0.0.0.255` )
  - `no auto-summary` (highly recommended for classless routing)
  - `passive-interface [interface_id]` (optional)
- **OSPFv2 (IPv4):**
  - `router ospf [process_id]` (e.g., `router ospf 1` )
  - `network [network_address] [wildcard_mask] area [area_id]` (e.g., `network 192.168.1.0 0.0.0.255 area 0` )
  - `router-id [ip_address]` (best practice)
  - `passive-interface [interface_id]` (optional)
  - `interface [interface_id]` (then: `ip ospf cost 4` )
- **OSPFv3 (IPv6):**
  - `ipv6 unicast-routing` (global command to enable IPv6 routing)
  - `ipv6 router ospf [process_id]`
  - `router-id [ip_address]`
  - `interface [interface_id]` (then: `ipv6 ospf [process_id] area [area_id]` )
- **BGP (Basic):**
  - `router bgp [local_asn]`
  - `neighbor [remote_ip_address] remote-as [remote_asn]`
  - `network [network_address] mask [subnet_mask]`

### III. Inter-VLAN Routing (Router-on-a-Stick)

- **Sub-interface Creation:**



- `interface [physical_interface_id].[vlan_id]` (e.g., `interface GigabitEthernet0/1.10` )
- `encapsulation dot1Q [vlan_id]`
- `ip address [ip_address] [subnet_mask]`

## IV. Access Control Lists (ACLs) - Definition

- **Standard ACL:**

- `access-list [number] permit [source] [wildcard_mask]` (e.g., `access-list 10 permit 192.168.1.0 0.0.0.255` )

- **Extended ACL:**

- `access-list [number] permit [protocol] [source] [wildcard_mask] [destination] [wildcard_mask]` (e.g., `access-list 100 permit tcp 192.168.1.0 0.0.0.255 any` )
- *Note: ACLs are applied to interfaces using `ip access-group [acl_number] {in | out}` .*

## V. Remote Management Security (SSH)

- `ip domain-name [domain]` (e.g., `ip domain-name example.com` )
- `crypto key generate rsa` (follow prompts for key size)
- `line vty 0 4`
- `transport input ssh`
- `username [username] privilege 15 secret [password]`

## VI. DHCP Server/Relay

- `ip dhcp pool [pool_name]`
- `network [network_address] [subnet_mask]`
- `default-router [router_ip]`
- `dns-server [dns_ip]`
- `ip dhcp excluded-address [start_ip] [end_ip]`
- `interface [interface_id]` (then: `ip helper-address [dhcp_server_ip]` )

## VII. WAN Connectivity

- **PPP with CHAP Authentication:**

- `interface [serial_interface_id]` (e.g., `interface Serial0/0` )
- `encapsulation ppp`
- `ppp chap hostname [username]` (e.g., `ppp chap hostname user123` )
- `ppp chap password [password]` (e.g., `ppp chap password MyPPPPassword` )
- `ppp authentication chap` (on the peer)

- **PPPoE Client:**

- `interface dialer [number]`
- `ip address negotiate`
- `encapsulation ppp`
- `dialer pool [number]`
- `dialer-group [number]`
- `ppp chap hostname [username_from_ISP]`
- `ppp chap password [password_from_ISP]`
- `interface [ethernet_interface_connected_to_modem]` (then: `pppoe-client dial-pool-number [dialer_pool_number]` )
- `dialer-list [number] protocol ip permit`

- **GRE VPN Tunnel:**

- `interface tunnel [number]` (e.g., `interface tunnel 1` )
- `ip address [ip_address] [subnet_mask]` (e.g., `ip address 10.1.1.1 255.255.255.0` )
- `tunnel source [source_ip]` (e.g., `tunnel source 192.168.1.1` )
- `tunnel destination [destination_ip]` (e.g., `tunnel destination 192.168.2.1` )
- `tunnel mode gre ip`

## VIII. NAT (Network Address Translation)

- `interface [interface_id]` (then: `ip nat inside` or `ip nat outside` )

- `ip nat inside source static [local_ip] [global_ip]` (e.g., `ip nat inside source static 192.168.1.10 203.0.113.1` )
- `ip nat pool [pool_name] [start_ip] [end_ip] netmask [subnet_mask]`
- `ip nat inside source list [acl_number] pool [pool_name]` (for dynamic NAT)
- `ip nat inside source list [acl_number] interface [outside_interface_id] overload` (for PAT/NAT Overload)

## IX. Quality of Service (QoS)

- `class-map [class_name]` (then: `match ...` )
- `policy-map [policy_name]`
- `class [class_name]` (then: `bandwidth [amount]` or `police ...` etc.)
- `interface [interface_id]` (then: `service-policy {input | output} [policy_name]` )

## X. IP SLA (Service Level Agreement)

- `ip sla [operation_number]` (e.g., `ip sla 1` )
- `icmp-echo [ip_address]` (e.g., `icmp-echo 8.8.8.8` )
- `frequency [seconds]` (e.g., `frequency 30` )
- `ip sla schedule [operation_number] life forever start-time now`
- `track [track_number] ip sla [operation_number] reachability`

## C. Switch Commands

These commands are primarily used for Layer 2 functionality, VLAN management, spanning tree, link aggregation, and first-hop redundancy.

### I. VLAN & Trunking Configuration

- `vlan [vlan_id]` (e.g., `vlan 10` )
- `name [vlan_name]`
- `interface [interface_id]` (e.g., `interface GigabitEthernet0/1` )
- `switchport mode access`
- `switchport access vlan [vlan_id]` (e.g., `switchport access vlan 10` )

- **Trunking Modes (on inter-switch links or to router sub-interfaces):**

- `switchport mode dynamic auto`
- `switchport mode dynamic desirable`
- `switchport mode trunk`
- `switchport nonegotiate` (used with `switchport mode trunk` to disable DTP)
- `switchport trunk encapsulation dot1Q` (if not default)
- `switchport trunk allowed vlan [vlan_list]`
- `switchport trunk native vlan [vlan_id]`

## II. VTP (VLAN Trunking Protocol)

- `vtp mode {server | client | transparent}` (e.g., `vtp mode server` )
- `vtp domain [domain_name]` (e.g., `vtp domain MyVTPDomain` )
- `vtp password [password]` (e.g., `vtp password VTPPassword123` )

## III. Spanning Tree Protocol (STP)

- `spanning-tree mode rapid-pvst` (or `pvst` for legacy)
- `spanning-tree vlan [vlan_id] priority [value]` (e.g., `spanning-tree vlan 10 priority 4096` )
- `spanning-tree vlan [vlan_id] root {primary | secondary}`
- `interface [interface_id]` (then: `spanning-tree link-type point-to-point` or `shared` )
- `spanning-tree portfast` (on access ports connected to end devices)
- `spanning-tree bpduguard enable` (on access ports with portfast)
- `clear spanning-tree detected-protocols`

## IV. EtherChannel (Link Aggregation)

- `interface port-channel [number]` (e.g., `interface port-channel1` )
- `switchport mode trunk` (or access, depending on role)
- `interface [physical_interface_id]` (e.g., `interface GigabitEthernet0/1` or `interface Range G0/1 - 2` )
- `channel-group [number] mode {on | active | passive | desirable | auto}`

## V. First-Hop Redundancy Protocols (FHRP)

- **HSRP (Hot Standby Router Protocol):**
  - `interface [interface_id]` (SVI or Layer 3 port)
  - `standby [group_number] ip [virtual_ip]` (e.g., `standby 1 ip 192.168.1.254` )
  - `standby [group_number] priority [priority_value]` (e.g., `standby 1 priority 100` )
  - `standby [group_number] preempt`
  - `standby [group_number] track [interface_id] [decrement_value]`

## VI. Switched Virtual Interfaces (SVIs)

- `interface vlan [vlan_id]`
- `ip address [ip_address] [subnet_mask]`
- `no shutdown`
- *Note: SVIs are essential for inter-VLAN routing on Layer 3 switches. ACLs can be applied to SVIs using `ip access-group` .*

## VII. Port Security

- `interface [interface_id]`
- `switchport mode access`
- `switchport port-security`
- `switchport port-security maximum [number_of_MACs]`
- `switchport port-security violation {shutdown | restrict | protect}`
- `switchport port-security mac-address {sticky | [mac_address]}`

## VIII. SNMP (Simple Network Management Protocol)

- `snmp-server community [community_string] ro` (Read-Only, e.g., `snmp-server community MyCommunityString ro` )
- `snmp-server community [community_string] rw` (Read-Write - use with caution)
- `snmp-server host [host_ip] traps [community_string]`

- `snmp-server enable traps [trap_type]`

## IX. Local SPAN (Port Mirroring)

- `monitor session [session_number] source interface [interface_id] {rx | tx | both}`
- `monitor session [session_number] destination interface [interface_id]`

This organization should provide a much clearer picture of where each configuration command fits within the context of router and switch functions.

## Router1 Configuration Example

### Goal:

- Basic device setup (hostname, passwords, SSH).
- WAN interface (Gig0/0) with a static public IP (simplified for example).
- LAN interface (Gig0/1) as a trunk for "Router-on-a-Stick" inter-VLAN routing.
- DHCP server for VLAN 10 and VLAN 20.
- Basic default route to the Internet.
- NAT (PAT) for internal networks to access the Internet.

### Code snippet

```
! Enter Global Configuration Mode
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
! --- Basic Setup & Security ---
Router(config)#hostname Router1
```

```
! Enable secret (stronger password for privileged EXEC mode)
Router1(config)#enable secret ciscoenablesecret
```

```
! Console password
Router1(config)#line con 0
```

```

Router1(config-line)#password ciscoconsole
Router1(config-line)#login
Router1(config-line)#logging synchronous
Router1(config-line)#exec-timeout 10 0
Router1(config-line)#exit

! VTY lines (SSH/Telnet access)
Router1(config)#line vty 0 4
Router1(config-line)#password ciscovty
Router1(config-line)#login
Router1(config-line)#transport input ssh
Router1(config-line)#exec-timeout 10 0
Router1(config-line)#exit

! Service password encryption (to encrypt type 7 passwords)
Router1(config)#service password-encryption

! SSH Configuration
Router1(config)#ip domain-name example.com
Router1(config)#crypto key generate rsa
! Choose a key size of 1024 or 2048 (e.g., 1024)
The name for the keys will be: Router1.example.com
Keys will be regenerated during mid-cycle config merges.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (Ended with CRLF)
Router1(config)#username admin privilege 15 secret adminpassword
Router1(config)#exit

! --- WAN Interface Configuration (GigabitEthernet0/0) ---
Router1#configure terminal
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#description Connection to ISP
Router1(config-if)#ip address 203.0.113.2 255.255.255.252 ! Example public IP /30
Router1(config-if)#no shutdown
Router1(config-if)#ip nat outside ! Mark as outside interface for NAT
Router1(config-if)#exit

! --- LAN Interface Configuration (GigabitEthernet0/1) - Router-on-a-Stick ---
Router1(config)#interface GigabitEthernet0/1
Router1(config-if)#description Trunk to Switch1
Router1(config-if)#no ip address
Router1(config-if)#no shutdown
Router1(config-if)#exit

Router1(config)#interface GigabitEthernet0/1.10
Router1(config-subif)#description Sales VLAN 10 Gateway
Router1(config-subif)#encapsulation dot1Q 10
Router1(config-subif)#ip address 192.168.10.1 255.255.255.0
Router1(config-subif)#ip nat inside ! Mark as inside for NAT
Router1(config-subif)#exit

```

```
Router1(config)#interface GigabitEthernet0/1.20
Router1(config-subif)#description Marketing VLAN 20 Gateway
Router1(config-subif)#encapsulation dot1Q 20
Router1(config-subif)#ip address 192.168.20.1 255.255.255.0
Router1(config-subif)#ip nat inside ! Mark as inside for NAT
Router1(config-subif)#exit
```

! --- DHCP Server Configuration ---

```
Router1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
Router1(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.9
```

```
Router1(config)#ip dhcp pool Sales_Pool
Router1(config-dhcp)#network 192.168.10.0 255.255.255.0
Router1(config-dhcp)#default-router 192.168.10.1
Router1(config-dhcp)#dns-server 8.8.8.8 8.8.4.4
Router1(config-dhcp)#lease 0 8 0 ! 8 hour lease
Router1(config-dhcp)#exit
```

```
Router1(config)#ip dhcp pool Marketing_Pool
Router1(config-dhcp)#network 192.168.20.0 255.255.255.0
Router1(config-dhcp)#default-router 192.168.20.1
Router1(config-dhcp)#dns-server 8.8.8.8 8.8.4.4
Router1(config-dhcp)#lease 0 8 0
Router1(config-dhcp)#exit
```

! --- Default Route & NAT (PAT/Overload) ---

```
! Default route pointing to ISP's gateway (203.0.113.1)
Router1(config)#ip route 0.0.0.0 0.0.0.0 203.0.113.1
```

! Access-list to identify "inside" traffic for NAT

```
Router1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
Router1(config)#access-list 1 permit 192.168.20.0 0.0.0.255
```

! Apply NAT Overload (PAT) using the WAN interface's IP

```
Router1(config)#ip nat inside source list 1 interface GigabitEthernet0/0 overload
```

! --- Save Configuration ---

```
Router1(config)#end
Router1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

## Router1 Verification Commands:

### Code snippet

```
Router1#show ip interface brief
! Verify IP addresses, sub-interfaces, and status (up/up)
```

```
Router1#show ip route
! Verify static default route and connected routes
```



```
Router1#show ip dhcp binding
! Check DHCP lease assignments after clients connect
```

```
Router1#show ip dhcp server statistics
! Check DHCP server activity
```

```
Router1#show ip nat translations
! Verify NAT translation entries as internal hosts browse the internet
```

```
Router1#show running-config
! Review the entire configuration
```

---

## Switch1 Configuration Example

### Goal:

- Basic device setup (hostname, passwords, SSH).
- Create VLANs.
- Configure trunking to Router1.
- Assign access ports to VLANs.
- Configure STP for rapid convergence.
- Implement port security on access ports.
- Configure a management IP (SVI) for remote access.

### Code snippet

```
! Enter Global Configuration Mode
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
! --- Basic Setup & Security ---
Switch(config)#hostname Switch1
```

```
! Enable secret
Switch1(config)#enable secret ciscoenablesecret
```

```
! Console password
Switch1(config)#line con 0
Switch1(config-line)#password ciscoconsole
Switch1(config-line)#login
Switch1(config-line)#logging synchronous
Switch1(config-line)#exec-timeout 10 0
Switch1(config-line)#exit
```

! VTY lines (SSH/Telnet access)

```
Switch1(config)#line vty 0 4
Switch1(config-line)#password ciscovty
Switch1(config-line)#login
Switch1(config-line)#transport input ssh
Switch1(config-line)#exec-timeout 10 0
Switch1(config-line)#exit
```

! Service password encryption

```
Switch1(config)#service password-encryption
```

! SSH Configuration (same as router, required if using SSH for switch management)

```
Switch1(config)#ip domain-name example.com
Switch1(config)#crypto key generate rsa
! Choose a key size of 1024 or 2048 (e.g., 1024)
The name for the keys will be: Switch1.example.com
Keys will be regenerated during mid-cycle config merges.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (Ended with CRLF)
Switch1(config)#username admin privilege 15 secret adminpassword
Switch1(config)#exit
```

! --- VLAN Creation ---

```
Switch1(config)#vlan 10
Switch1(config-vlan)#name Sales
Switch1(config-vlan)#exit
```

```
Switch1(config)#vlan 20
Switch1(config-vlan)#name Marketing
Switch1(config-vlan)#exit
```

! --- Management SVI (VLAN 99 for management, common practice) ---

```
Switch1(config)#vlan 99
Switch1(config-vlan)#name Management
Switch1(config-vlan)#exit
```

```
Switch1(config)#interface vlan 99
Switch1(config-if)#description Switch Management Interface
Switch1(config-if)#ip address 192.168.99.10 255.255.255.0 ! Example IP
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
```

! Default Gateway for Switch Management (to reach Router1)

```
Switch1(config)#ip default-gateway 192.168.99.1 ! Assuming Router1 will also have a G0/1.99 SVI or L3 port
! (This is not in Router1 config above, but would be needed)
! Router1(config-subif)#interface GigabitEthernet0/1.99
! Router1(config-subif)#encapsulation dot1Q 99
! Router1(config-subif)#ip address 192.168.99.1 255.255.255.0
```

! --- Trunk Port Configuration (to Router1) ---

```

Switch1(config)#interface GigabitEthernet0/1
Switch1(config-if)#description Uplink to Router1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#switchport trunk native vlan 99 ! Example native VLAN, could be any unused VLAN
Switch1(config-if)#switchport trunk allowed vlan 10,20,99 ! Allow only necessary VLANs
Switch1(config-if)#no shutdown
Switch1(config-if)#exit

! --- Access Port Configuration ---
! Port for PC1 (Sales)
Switch1(config)#interface GigabitEthernet0/2
Switch1(config-if)#description PC1_Sales
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#spanning-tree portfast ! Fast-forwarding for end devices
Switch1(config-if)#switchport port-security ! Enable port security
Switch1(config-if)#switchport port-security maximum 1 ! Allow only 1 MAC address
Switch1(config-if)#switchport port-security violation restrict ! Drop traffic & log, but don't shut down port
Switch1(config-if)#no shutdown
Switch1(config-if)#exit

! Port for PC2 (Marketing)
Switch1(config)#interface GigabitEthernet0/3
Switch1(config-if)#description PC2_Marketing
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
Switch1(config-if)#spanning-tree portfast
Switch1(config-if)#switchport port-security
Switch1(config-if)#switchport port-security maximum 1
Switch1(config-if)#switchport port-security violation restrict
Switch1(config-if)#no shutdown
Switch1(config-if)#exit

! --- Spanning Tree Protocol (STP) Configuration ---
Switch1(config)#spanning-tree mode rapid-pvst
Switch1(config)#spanning-tree vlan 1,10,20,99 root primary ! Make this switch the root for these VLANs
! (Assuming it's the central distribution switch)
! Optional: configure a secondary root for redundancy
! Switch1(config)#spanning-tree vlan 1,10,20,99 root secondary

! --- Save Configuration ---
Switch1(config)#end
Switch1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

## Switch1 Verification Commands:

Code snippet

---

Switch1#show vlan brief  
! Verify VLANs are created and ports are assigned correctly

Switch1#show interfaces trunk  
! Verify Gig0/1 is a trunk and carrying the correct VLANs

Switch1#show interface status  
! Check port status and VLAN assignment

Switch1#show spanning-tree summary  
! Verify rapid-pvst mode and root bridge status

Switch1#show spanning-tree vlan 10  
! Detailed STP status for a specific VLAN

Switch1#show port-security  
! Check global port security status

Switch1#show port-security interface GigabitEthernet0/2  
! Check port security status for a specific interface

Switch1#show ip interface brief  
! Verify SVI IP address

Switch1#show ip default-gateway  
! Verify the configured default gateway

Switch1#show running-config  
! Review the entire configuration

---

## Next Steps After Configuration:

1. **Connect Devices:** Plug in the physical cables according to the diagram.
2. **Power On:** Ensure all devices are powered on.
3. **Client Configuration:**
  - Set PCs (PC1, PC2) to obtain IP addresses automatically via DHCP.
  - Verify they receive IPs from the correct VLAN range and can ping their default gateway (Router1's sub-interface IP).
4. **Test Connectivity:**
  - Ping between PCs in the same VLAN.
  - Ping between PCs in different VLANs (should work via Router1).
  - Ping to the Internet (e.g., `ping google.com` ).

- Test SSH access to both Router1 and Switch1 from a management PC.

This comprehensive example covers many of the topics you listed, providing a practical demonstration of how to apply the commands. Remember to adjust IP addresses, VLAN IDs, passwords, and interface names to match your specific lab or production environment.